REMARKS

Claims 18-29 have been canceled. Claims 1, 3, 12, 16, 30, and 32 have been amended to clarify the subject matter regarded as the invention. Claim 33 has been added. Claims 1-17 and 30-33 remain pending.

Applicants affirm the election of Group I, claims 1-17 and 30-32.

The Examiner states that the provisional applications upon which priority is claimed fail to provide adequate support for claims 1-17 and 30-32 of the present application under 35 U.S.C. 112.

Applicants believe U.S. Provisional Patent Application No. 60/143,821 provides adequate support for the claims. See, e.g., pages 3, 5-7, and 9-11. On pages 5, 6, and 9-11, automatically generating content for a computer is described, including how the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version of a system such as the intruder would expect to see upon gaining unauthorized access to the computer. On page 7, creating on the computer a deception environment comprising a fully functional operating system and the automatically generated content is described. Determining automatically based on a preconfigured policy not specific to any user whether a user should be routed to the deception environment is described on page 3 (second paragraph). On page 2 (step 3), page 3 (second paragraph), and page 4 (first bullet), routing the user to the deception environment if it is determined that the user should be routed to the deception environment is described. It is therefore believed that the Applicant's claim for domestic priority under 35 U.S.C. 119(e) to U.S. Provisional Patent Application No. 60/143,821 is proper.

Applicants believe U.S. Provisional Patent Application No. 60/151,531 provides adequate support for the claims. See, e.g., pages 3-7. On pages 4 and 5-7, automatically generating content for a computer is described, including how the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version of a system such as the intruder would expect to see upon gaining unauthorized access to the computer. On page 4 ("The Cage"), creating on the computer a deception environment comprising a fully functional operating system and the automatically generated content is

described. Determining automatically based on a preconfigured policy not specific to any user whether a user should be routed to the deception environment is described on page 3 (bottom). On page 3 (bottom), routing the user to the deception environment if it is determined that the user should be routed to the deception environment is described. It is therefore believed that the Applicant's claim for domestic priority under 35 U.S.C. 119(e) to U.S. Provisional Patent Application No. 60/151,531 is proper.

The Examiner has indicated that the drawings are objected to as failing to comply with 37 CFR 1.84(g), 37 CFR 1.84(l), and 37 CFR 1.84(p)(5). It is believed that the attached formal drawings overcome the objections to the drawings.

The Examiner has rejected claim 3 under 35 U.S.C. 112, second paragraph. Claim 3 has been amended to overcome the rejection.

The Examiner has rejected claims 1-3, 5-11, 14-17, and 30-32 under 35 U.S.C. 102(b) as being anticipated by Cheswick.

The rejection is respectfully traversed. With respect to claim 1, Cheswick describes connecting a known hacker with the account name "berferd" to a jail that attempts to present to the hacker an environment that leads the intruder to believe the hacker is connected to the computer the hacker is targeting.

Claim 1 recites "automatically generating content for a computer associated with the network." In contrast, Cheswick describes the manual creation of content. "The scripts we used, and for that matter the Jail itself, were created on the fly." (see "Berferd Comes Home") In addition, manual creation of deception environment content is slow and risks detection due to errors and lack of completeness. Cheswick describes how "the jail was hard to set up" and "we had to be careful to keep errors in the setup scripts from the hacker's eyes." (see "The Jail") Using the approach disclosed by applicants and recited in claim 1, whereby content is generated automatically, avoids the disadvantages of the manual approach taught by Cheswick because a complete file system can be generated quickly without risk of human error. See Application p. 23, line 3 – p. 27, line 19; and p. 29, lines 1-7.

In addition, Cheswick does not describe how "the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version

of a system such as the intruder would expect to see upon gaining unauthorized access to the computer," as recited in amended claim 1. See Application p. 29, lines 1-7. Cheswick admits the jail he describes is "not undetectable" and that "there were errors, things that could have tipped off Berferd, had he been more alert" (see "The Jail" and "Berferd Comes Home").

Cheswick also does not describe "creating on the computer a deception environment comprising a fully functional operating system," as recited in amended claim 1. Cheswick describes how "several raw disk files were too dangerous to leave around. We removed ps, who, w, netstat, and other revealing programs." (see "The Jail") While Cheswick teaches removing revealing programs, including ps, a program used to display current processes, the Application describes copying a fully functional operating system into the deception environment, as recited in claim 1, and filtering requests, such as requests invoking the ps program or its equivalent (e.g., proc), to hide processes that might tip the intruder off to the fact that he/she is being monitored. Application p. 32, lines 12-22. In this way, a fully functional operating system is included in the deception environment, and no functionality of the operating system is omitted or removed to prevent detection.

Finally, Cheswick describes configuring the berferd account and a guest account to connect to the jail (see "The Jail"), but does not describe "determining automatically based on a preconfigured policy *not specific to any user* whether a user should be routed to the deception environment," as recited in amended claim 1 (italics added). Support for this amendment may be found, without limitation, in the above-captioned application at page 18, lines 16 to page 19, line 10.

For the reasons described above, claim 1 is believed to be allowable over Cheswick.

The Examiner has rejected claims 1, 4, 12, and 13 under 35 U.S.C. 102(b) as being anticipated by Green et al.

The rejection is respectfully traversed. With respect to claim 1, Green describes binding processes associated with an administrative server to an internal burb and binding the processes associated with a commerce server to an external burb, where a burb is a protocol stack with all the processes that can access that stack. An attacker who gains control of the external burb is prevented from accessing the internal burb. Green does not describe "automatically generating

content for a computer associated with the network," as recited in claim 1. Nor does Green describe "creating on the computer a deception environment comprising a fully functional operating system and the automatically generated content," as recited in amended claim 1. As such, claim 1 is believed to be allowable over Green.

Claims 2-17, and new claim 33 depend from claim 1 and are believed to be allowable for the same reasons described above.

Like claim 1, claims 30 and 32 recite providing security for a computer network including "automatically generating content for a computer associated with the network, creating on the computer a deception environment comprising a fully functional operating system and the automatically generated content, determining automatically based on a preconfigured policy not specific to any user whether a user should be routed to the deception environment, and routing the user to the deception environment if it is determined that the user should be routed to the deception environment, wherein the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version of a system such as the intruder would expect to see upon gaining unauthorized access to the computer." As such, claims 30 and 32 are believed to be allowable.

Claim 31 depends from claim 30 and is believed to be allowable for the same reasons described above.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Clover Huang

Clover Huang
Registration No. 55,285
V 408-973-2594
F 408-973-2595

VAN PELT AND YI, LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014